ELSEVIER

Discrete Mathematics 148 (1996) 175–204

DISCRETE MATHEMATICS

Codes and Siegel modular forms

Bernhard Runge

Fakultät für Mathematik und Informatik, Universität Mannheim, 68131 Mannheim Germany

Received 1 December 1992; revised 15 March 1994

Abstract

It is proved that the ring of Siegel modular forms in any genus is determined by doubly even self-dual codes and the theta relations. The (higher) weight polynomials of such codes are proved to be the generators of the ring of invariants of a polynomial ring in 2^g variables under a certain specified finite group. Moreover codes are uniquely determined by their weight polynomials.

1. Introduction

The word *code* is used to mean a binary linear code, i.e. a linear subspace C of $\boldsymbol{F}_2^n$ of dimension k, denoted $[n,k,d]$. Here d is used to denote the minimal weight $d = \min\{|\alpha| \text{ with } \alpha \in C\backslash\{0\}\}$. The *weight* $|\alpha|$ is just the number of entries 1 in a codeword α and is used as a number in $\mathbb{Z}$ or in $\boldsymbol{F}_2$. The vectors in C are also called codewords. The number n is called the length of the code. On $\boldsymbol{F}_2^n$ we have the componentwise product of elements and the usual inner product with $\langle x, y\rangle = |xy|$ and $x = xx$. We denote as usual the element $0 = (0,\ldots,0)$ and $1 = (1,\ldots,1)$. The dual code $C^\perp$ refers to the orthogonally complementary subspace. A code is self-dual when it coincides with its dual. There is the obvious formula

$$|x + y| = |x| + |y| - 2|xy|.$$

A code is called *even* iff the weight of every codeword is divisible by 2. A code is called *doubly-even* iff the weight of every codeword is divisible by 4. By the just mentioned formula a doubly-even code has the property $C \subset C^\perp$. A code is usually given by a basis written as a matrix like the following examples:

$$Rep_n = \begin{bmatrix} 0 & \cdots & 0 \\ 1 & \cdots & 1 \end{bmatrix} = \{0, 1\}$$

SSDI 0012-365X(94)00271-1

is a $[n,1,n]$-code (usually called repetition code) or

$$C_1 = \begin{bmatrix} 0\,0\,1\,1 \\ 1\,1\,0\,0 \end{bmatrix}$$

is the unique $[4,2,2]$-code if one considers (as we will always do) two codes as equivalent if there is a permutation in S_n, which maps one code to the other. A self-dual code always contains the code Rep_n.

One calls $Aut(C) = \{\sigma \in S_n \text{ with } \sigma(C) = C\}$ the automorphism group of the code. Other examples are the (unique) $[n, n-1, 2]$-code $Rep_n^{\perp}$ (sum zero or parity check code) or the $[n,n,1]$-code $(C = \boldsymbol{F}_2^n)$.

The most interesting self-dual codes have the further property of being doubly-even. Self-dual doubly-even codes only exist in length a multiple of 8 (or $k = \dim(C) = n/2$ a multiple of 4).

There are more interesting examples as above like the (unique) self-dual doubly-even $[8,4,4]$-code H_8 called Hamming code with a generator matrix like

$$H_8 = \begin{pmatrix} & & & 1 & 1 & 1 & 1 \\ & & 1 & 1 & & 1 & 1 \\ & 1 & 1 & 1 & 1 & & \\ 1 & & 1 & & 1 & & \end{pmatrix}$$

or the (unique) self-dual doubly-even $[24,12,8]$-code G_{24} called Golay code, see [P] or Appendix 5 in [28].

In the papers [3,30,29] self-dual doubly-even codes up to length 32 are classified. The method is always to glue the code together from easier subcodes. Especially, the 4-words or tetrads or the subcode generated by 4-words are studied. After classifying the tetrads one regards the possible extensions by gluing vectors. These methods are very successful for small codes. For example, it is easy to get the list of the nine self-dual doubly-even codes in length 24, in length 32 there are already 85 codes [3]. There is an obvious notion of direct product of codes and indecomposable codes. Of course, only the indecomposable codes are interesting if one wants to classify codes.

We need later the formula

$$\#\left\{ \begin{array}{c} \text{self-dual doubly-even} \\ \text{codes in length } 2n \end{array} \right\} = 2 \cdot 3 \cdots (2^{n-3}+1) \cdot (2^{n-2}+1)$$

which follows from the more general theorem in [26] that for any doubly-even $[n,s,d]$-code T with $8|n$ and $1 \in T \subset T^{\perp}$ (weakly self-dual) the number of (doubly-even self-dual) codes C which contain T is

$$2 \cdot 3 \cdots (2^{n/2-s-2}+1) \cdot (2^{n/2-s-1}+1).$$

As an application of this formula one may conclude that $H_8 \times H_8$ and

$$D_{16}^{+} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & \cdots \\ & & 1 & 1 & 1 & 1 & \cdots \\ \vdots & \vdots & & \ddots & & & \vdots \\ 1 & & 1 & & 1 & \cdots\cdots & \end{pmatrix}$$

are the only self-dual doubly-even codes in length 16 (see [3]).

Lemma. *A $d \times 2d$-matrix of type $(1, M)$ is a generator matrix of a self-dual doubly-even code iff*

$$MM^{t} \equiv 1 \bmod(2) \text{and } \operatorname{diag}(MM^{t}) \equiv 3 \bmod(4).$$

Proof. A matrix of the given type has rank d. The first condition means that any two vectors of the basis are orthogonal, which implies $C \subset C^{\perp}$; hence together with the dimension $C = C^{\perp}$. The condition for the diagonal implies that the basis vectors have weight divisible by 4 which gives doubly-even by induction due to the formula $|x + y| = |x| + |y| - 2|xy|$. The other direction is obvious. □

For a code C in length n one defines the weight polynomial as

$$\mathcal{W}_C(x, y) = \sum_{\alpha \in C} x^{n-|\alpha|} y^{|\alpha|}.$$

There is a definition of biweight polynomial in [13]. We give now a general definition for a gth-weight polynomial. We define for any $a \in \boldsymbol{F}_2^g$ a function on $\underbrace{C \times C \times \cdots C}_{g} \subset$ $\underbrace{\boldsymbol{F}_2^n \times \boldsymbol{F}_2^n \times \cdots \boldsymbol{F}_2^n}_{g} = (\boldsymbol{F}_2^n)^g$ as

$$a(\alpha_1, \ldots, \alpha_g) = \#\{i \text{ with } a = (\alpha_{1,i}, \ldots, \alpha_{g,i})\}.$$

Then we get the gth-weight polynomial as

$$P_g(C) = \sum_{\alpha_1, \ldots, \alpha_g \in C} \prod_{a \in \boldsymbol{F}_2^g} f_a^{a(\alpha_1, \ldots, \alpha_g)}.$$

The gth-weight polynomial P_g is considered as a polynomial in

$$B_g = \mathbb{C}[f_a \text{ with } a \in \boldsymbol{F}_2^g].$$

One has

$$P_1(C) = \mathcal{W}_C.$$

The gth-weight polynomials are closely connected to the theory of modular forms. This will be the main theme of the paper. We call the number g the *genus* of the weight polynomial. We prove that codes are uniquely determined by their weight polynomials.

Moreover, the ring of Siegel modular forms (for the full modular group in weight divisible by 4) is the normalization of a homomorphic image of the ring generated by the weight polynomials of doubly-even self-dual codes. Hence, from an algebraic point of view, the theory of modular forms is just coding theory plus the study of the theta relations. In genus one and two there are no relations, in genus three there is one relation and for higher genus it is an open problem to determine the ideal of theta relations.

All of the theory can be easily generalized for codes over other finite fields or modules over $\mathbb{Z}/n$, etc. The restriction to $\boldsymbol{F}_2$ is only chosen for simplicity.

2. Siegel modular forms

Throughout the paper we will use the following notations in accordance with [33,34]. General references are [8,16,25,27,31,39]:

$$\mathbb{H}_g = \{z \in Mat_{g\times g}(\mathbb{C}) | z \text{ symmetric}, \quad \mathrm{Im}(z) > 0\},$$
$$\Gamma_g = Sp(2g, \mathbb{Z}),$$
$$\Gamma_g(n) = \mathrm{Ker}(\Gamma_g \to Sp(2g, \mathbb{Z}/n)).$$

For a subgroup of finite index $\Gamma \subset \Gamma_g$, we denote by $A(\Gamma) = \bigoplus_k [\Gamma, k]$ the ring of modular forms for Γ. The ring $A(\Gamma)$ is a normal graded integral domain finitely generated as algebra over $\mathbb{C} = [\Gamma, 0]$. The variety $\mathcal{A}_g(\Gamma) = \mathrm{Proj}(A(\Gamma))$ is called Satake compactification of level Γ.

The thetas of second order are given by (we use Mumford's notation f_a)

$$f_a(\tau) = \theta \begin{bmatrix} a \\ 0 \end{bmatrix} (2\tau) = \sum_{x \in \mathbb{Z}^g} \exp 2\pi i(\tau[x + \tfrac{1}{2}a])$$

for $a \in \mathbb{Z}^g$. The functions f_a only depend on a mod 2 hence a is regarded as element in $\boldsymbol{F}_2^g$. We recall from [33] that the ring of modular forms of even weight is given by

$$\bigoplus_{2|k} [\Gamma_g, k] = (\mathbb{C}[f_a]^{H_g})^N,$$

where N denotes the normalization in its field of fractions and H_g is a finite group. (Here the f_a have to be read as thetas.) The Siegel Φ-operator may be defined analytically. For Siegel modular forms in even weight (which are always rational functions in the theta constants of second order) the Φ-operator is given by

$$\Phi(f_{\binom{a}{0}}) = f_a \quad \text{and} \quad \Phi(f_{\binom{a}{1}}) = 0.$$

(Here a is considered as element in $\boldsymbol{F}_2^g$ and $\binom{a}{*}$ as an element in $\boldsymbol{F}_2^{g+1}$.)

It is well known that the group Γ_g is generated by

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix},$$

where S runs over all symmetric $g \times g$-matrix (1 is the 1 in $\mathrm{Gl}(g,\mathbb{Z})$). The action of the modular group on the thetas of second order is given by:

$$\sigma = \begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix}$$

acts by $\sigma(f_a) = i^{S[a]} f_a$ and $\sigma = J$ acts as follows: Let

$$T_g = \left(\frac{1+i}{2}\right)^g \left((-1)^{\langle a,b\rangle}\right)_{a,b\in \boldsymbol{F}_2^g},$$

a scalar multiple of a square matrix with entries ± 1, then

$$\frac{J(f_a)}{\sqrt{\det(-\tau)}} = \sum_{b\in \boldsymbol{F}_2^g} (T_g)_{a,b} f_b$$

holds for all $a \in \boldsymbol{F}_2^g$. This is a matrix equation, which is independent of the choice of the square root on the 2-ring, i.e. on the ring $\mathbb{C}[f_a f_b] = \{f \in B_g \text{ with } 2|\deg(f)\}$. (The correct square root is $\sqrt{\det(\tau/i)}$ which is here replaced by $\varepsilon^g\sqrt{\det(-\tau)}$ with $\varepsilon = (1+i)/\sqrt{2}$ a primitive 8th root of unity, see [8]. We use the equation only for mixed products, hence we are doing nothing wrong.) Take $D_S = \mathrm{diag}(i^{S[a]} \text{ for } a \in \boldsymbol{F}_2^g)$ and let

$$H_g = \langle T_g, D_S \rangle$$

be the subgroup of $\mathrm{Gl}(2^g,\mathbb{C})$ generated by the elements T_g and D_S. If we map J to T_g and

$$\begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix}$$

to D_S we get a (surjective) homomorphism of groups

$$\phi : \Gamma_g \longrightarrow H_g/(\pm 1).$$

We gave a description of the kernel denoted by $\Gamma_g^*(2,4)$ in [33]. We use the elements $P_S = T_g^7 D_S^2 T_g$ in the following lemma, D_S is already defined.

Let $0,1,2,3,\ldots 2^g - 1$ identify with $\boldsymbol{F}_2^g$ via the binary number representation, i.e.

$$0 = 0,0,\ldots 0, \qquad 1 = 0,0,\ldots 1,$$

$$2 = 0,\ldots 1,0, \qquad 3 = 0,\ldots 1,1,$$

etc. This identification will be used frequently. The first application is as follows. We take the affine linear group

$$AGl(g) := \boldsymbol{F}_2^g \times \mathrm{Gl}(g, \boldsymbol{F}_2)$$

together with the standard action of $AGl(g)$ on $\boldsymbol{F}_2^g$ given by $(x,M)(a) = Ma + x$. The group $AGl(g)$ will be considered as a subgroup in $Gl(2^g, \mathbb{C})$ just by permuting the f_a. It is shown in [33] that we get an inclusion

$$AGl(g) \subset H_g \subset \mathrm{Gl}(2^g, \mathbb{C}).$$

We introduced in [33] the following elements. We replace the (i,i)-coefficient in 0_g with 1 and call the matrix S. Then $E_i = D_S$ for this special S. Let $P_i = T_g^7 E_i^2 T_g$ and $M_i = (-1)^g (T_g E_i)^3 T_g$. Then $M_i^2 = i$. M_i is a modified MacWilliams identity in coding theory. The M_i are commuting with each other and its product gives back T_g.

Then $P_i(f_a) = f_{a+2^i}$ in the identification above. For $i \neq j$ we replace the (i,j)- and the (j,i)-coefficient in 0_g with 1 and call the matrix S, then $E_{ij} = D_S$. If $a \in \boldsymbol{F}_2^g$ is considered as a vector with entries 0 and 1 and if P_{ij} is the permutation matrix (ij) in $S_g \subset Gl(g, \boldsymbol{F}_2)$ then the following equation holds:

$$(-i) f_{P_{ij}a} = (M_i M_j E_{ij})^3 f_a.$$

Furthermore, one has for a nonvanishing linear form on $\boldsymbol{F}_2^g$ a corresponding embedding of $AGl(g-1)$ in $AGl(g)$ and (compatible with the following lemma) an embedding $H_{g-1} \subset H_g$. The embedding (A,x) going to

$$\left(\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} x \\ 0 \end{pmatrix} \right)$$

corresponds to the Siegel Φ-operator, i.e. the following diagram commutes:

$$\begin{array}{ccccc} H_g & \times & B_g & \longrightarrow & B_g \\ \triangle \uparrow & & \Phi \downarrow & & \Phi \downarrow \\ H_{g-1} & \times & B_{g-1} & \longrightarrow & B_{g-1} \end{array}$$

Lemma 2.1. *One has an exact sequence*

$$0 \to N_g \longrightarrow H_g \longrightarrow Sp(2g, \boldsymbol{F}_2) \to 0.$$

The group $N_g = \langle i, D_S^2, P_S \rangle$ with $\#N_g = 2^{2g+2}$ is a central extension of an extraspecial 2-group. The factor group $N_g/\langle i \rangle = \boldsymbol{F}_2^{2g}$ is an elementary abelian group, and the right homomorphism is given by the conjugation of H_g on this $\boldsymbol{F}_2$-vector space.

Proof. For the proof we give as general reference the book of Dornhoff [5]. It is proved there that the symplectic group is generated by symplectic transvections. Moreover, we use the chapter about extraspecial 2-groups. The general principle of proof is analogous to the proof of the Bruhat decomposition of a linear group. One proves a commutator lemma by reduction to the case of rank two. It comes out that in our case the reduction to the genus two case is enough and there the lemma is an easy check.

We introduced the elements P_i and E_i of order two and four for $i = 1 \ldots g$. It is easy to see that

$$P_s E_t P_s = \begin{cases} E_t & \text{if } s \neq t, \\ iE_t^3 & \text{else,} \end{cases}$$

$$P_s M_t P_s = M_t \iff s \neq t.$$

Hence,

$$[P_s, E_t^2] = \begin{cases} -1 & \text{if } s \neq t, \\ 1 & \text{else.} \end{cases}$$

Now it is easy to check that N_g is an extension of an extraspecial 2-group as described in [35] by using the results in [5]. The action of H_g by conjugation on N_g is for the generating elements given as above by a symplectic transvection. One may check that we get enough transvections and hence the surjectivity in the above sequence. □

The group H_g is generated by the elements P_i, M_i, E_i and E_{ij}. The first three are in the image of H_1 under the various embeddings which correspond to flags of subvector spaces of $\boldsymbol{F}_2^g$. The E_{ij} are in the image of H_2 under such embeddings. It holds that $H_g \cap S_{2^g} = AGl(g)$ inside $\mathrm{Gl}(2^g, \mathbb{C})$. All these statements are easily checked for genus $1, 2, 3$. The general case follows from that by using the various diagonal embeddings.

In [34,35] we described the groups more in detail. The sequence in Lemma 2.1 is nonsplit and remains nonsplit after dividing by $\langle i \rangle = Z(H_g)$. Moreover, it is the unique nonsplit sequence [20]. We will fix the notation

$$G_g = (H_g, \varepsilon) = (AGl(g), E, W),$$

with

$$E = \mathrm{diag}(1, i, 1, i, \ldots),$$

$$W = \begin{pmatrix} W_1 & 0 \\ 0 & \ddots \end{pmatrix}.$$

with 2^{g-1} blocks

$$W_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

along the diagonal. The equality of groups holds due to $(WE)^3 = \varepsilon$ and the relations in [34, Ch. 2]. For the ring of invariants we fix

$$CP_g = B_g^{G_g}.$$

(The notation is motivated by Theorem 3.6.) The Φ-operator $\Phi : CP_{g+1} \longrightarrow CP_g$ is surjective, see [35]. One may compute that $AGl(1) \cong S_2$, $AGl(2) \cong S_4$ and that for higher genus $AGl(g)$ is a subgroup of A_{2^g}. For instance, $AGl(3)$ has index 15 in A_8.

The groups G_g have a decomposition of Bruhat type (with respect to the parabolic subgroup $AGl(g)$, which corresponds to the set of shorter roots in the Dynkin diagram C_g of the symplectic group). Let

$$G_{g,\mathrm{mon}} = (H_{g,4}, \varepsilon) = \{\text{matrices in } G_g \text{ with } 2^g \text{ nonzero entries}\}$$

the monomial subgroup of G_g and $W^{\otimes i}$ defined by 2^{g-i} blocks $W_1^{\otimes i}$ (of size 2^i) along the diagonal (for example,

$$W^{\otimes 2} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

then

$$G_g = \uplus_{i=0..g} G_{g,\mathrm{mon}} W^{\otimes i} G_{g,\mathrm{mon}}$$

and the cells in this decomposition of Bruhat type are characterized by the property, that the number of the nonzero entries in the matrices is just $2^{g-i}4^i$.

Remark 2.2. One has an exact diagram

$$\begin{array}{ccccccc} 0 & \to & N_g & \longrightarrow & H_g & \longrightarrow & Sp(2g, \boldsymbol{F}_2) \to 0 \\ & & \cup & & \cup & & \cup \\ 0 & \to & \boldsymbol{F}_2^g & \longrightarrow & AGl(g) & \longrightarrow & Gl(g, \boldsymbol{F}_2) \to 0 \end{array}$$

The map on the right is given by

$$U \mapsto \begin{pmatrix} U & 0 \\ 0 & (U^{\mathrm{t}})^{-1} \end{pmatrix}.$$

We set $H_{g,4} = \langle AGl(g), i, D_S, P_S \rangle$ the monomial subgroup in H_g of index $1 \cdot 3 \cdots (2^g + 1)$. (We chose the notation $H_{g,4}$ because on the f_a^4 the action is only by permutation.) One may check

$$\phi(\Gamma_{g,0}(2)) = H_{g,4}/(\pm 1)$$

($\Gamma_{g,0}(2)$ is defined by the condition $C \equiv 0 \bmod(2)$ and usually called the Hecke subgroup of level 2)

$$\phi(\Gamma_g(2)) = N_g/(\pm 1).$$

Example 2.3. We have $\Gamma_1^*(2,4) = \Gamma_1(4)$ and

$$N_1 = \left\langle i, P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

is an extended Dieder-group of order 16. The group $G_1 = \langle W, E\rangle$ generated by

$$W = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad E = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

is a group generated by (pseudo) reflections of order 192. The vector space $(N_1, \varepsilon)/\varepsilon = \boldsymbol{F}_2^2$ is generated by P and $iWPW = E^2$, the symplectic form on $(N_1, \varepsilon)/\varepsilon$ is given by

$$f(x, y) = \begin{cases} 0 \text{ if } xy = yx, \\ 1 \text{ else.} \end{cases}$$

P, WPW is a symplectic basis and $Sp(2, \boldsymbol{F}_2) \cong S_3$. See also [2].

Remark 2.4. For genus 2 the groups are as follows:

$$Sp(4, \boldsymbol{F}_2) \cong S_6 \quad \text{and} \quad AGl(2, \boldsymbol{F}_2) \cong S_4.$$

For the convenience of the reader we recall the following facts about group orders:

$$\#AGl(g) = 2^g(2^g - 1)\cdots(2^g - 2^{g-1}),$$

$$\#Sp(2g, \boldsymbol{F}_2) = 2^{g^2}(4^g - 1)\cdots 3,$$

$$\#H_g = 2^{g^2+2g+2}(4^g - 1)\cdots 3,$$

$$\#H_{g,4} = 2^{g^2+2g+2}(2^g - 1)(2^{g-1} - 1)\cdots 3.$$

Remark 2.5. For genus three we have $AGl(3) \cong Aut(H_8)$. The order is $\binom{8}{2}3 \cdot 2^4 = 1344$. (The group acts threefold transitive on the eight variables. For any two positions (of the eight entries) there exist exactly three 4-words which one on the chosen positions. Moreover, for any two positions there is exactly one decomposition in four two blocks such that D_8 is a subcode with this block decomposition.) Hence, there are $30 = 8!/1344$ codes equivalent to H_8 in $\boldsymbol{F}_2^8$.

3. The MacWilliams identity and the H_g-action

We recall the definition of the gth-weight polynomial as

$$P_g(C) = \sum_{\alpha_1,\ldots,\alpha_g \in C} \prod_{a \in \boldsymbol{F}_2^g} f_a^{a(\alpha_1,\ldots,\alpha_g)}.$$

The polynomial $P_g(C)$ is considered as a polynomial in

$$B_g = \mathbb{C}[f_a \text{ with } a \in \boldsymbol{F}_2^g].$$

By using the binary number convention we regard B_g as the polynomial ring in the formal symbols $f_0, \ldots, f_{2^g-1}$. The weight polynomials as defined above are homogeneous

polynomials of degree

$$\deg(P_g(C)) = \text{length}(C)$$

and have the following obvious property.

3.1. Specialization formula

$$P_g(C)(XX_0, YX_0, XX_1, YX_1, \ldots) = P_{g-1}(C)(X_0, X_1, \ldots)P_1(C)(X, Y).$$

This may be translated in terms of modular forms. The restriction of a modular form to decomposable points corresponds to a Segre embedding. This is described in [34]. The specialization formula may be generalized for $g = r + s$ with the weight polynomials in genus g, r and s.
With the help of

$$\sum_{\alpha \in C} (-1)^{\langle \alpha, \beta \rangle} = \begin{cases} \#C \text{ if } \beta \in C^{\perp}, \\ 0 \quad \text{else.} \end{cases}$$

one gets the *MacWilliams identity.*

3.2. *For a self-dual* $[2d, d, *]$*-code* C *one has the identity*

$$P_g(C)(f_0 + f_1, f_0 - f_1, f_2 + f_3, \ldots) = 2^d P_g(f_0, f_1, f_2, \ldots).$$

Proof. The proof is elementary. The method is a finite analogue of the Fourier transformation. We denote for this proof by

$$P_{C_1, \ldots, C_g} = \sum_{\alpha_1 \in C_1, \ldots, \alpha_g \in C_g} \prod_{a \in \boldsymbol{F}_2^g} f_a^{a(\alpha_1, \ldots, \alpha_g)}$$

a generalization of the weight polynomial for g codes of length n with $P_{C, \ldots, C} = P_g(C)$. Now we compute

$$\begin{aligned} P_{C^{\perp}, C_2, \ldots, C_g} &= \sum_{\gamma \in C^{\perp}, \alpha_i \in C_i} \prod_{a \in \boldsymbol{F}_2^g} f_a^{a(\gamma, \ldots, \alpha_g)} \\ &= (\#C)^{-1} \sum_{\beta \in C, \alpha \in \boldsymbol{F}_2^n, \alpha_2 \in C_2, \ldots} (-1)^{\langle \alpha, \beta \rangle} \prod_{a \in \boldsymbol{F}_2^g} f_a^{a(\cdots)}. \end{aligned}$$

One may regard the inner product and the product over the f_a as product of the componentwise defined product and for any $a \in \boldsymbol{F}_2^g$ the characteristic function on $\underbrace{\boldsymbol{F}_2 \times \boldsymbol{F}_2 \times \cdots \boldsymbol{F}_2}_{g} = \boldsymbol{F}_2^g$ as

$$a(\alpha_1, \ldots, \alpha_g) = \begin{cases} 1 \text{ if } a = (\alpha_1, \ldots, \alpha_g), \\ 0 \text{ else.} \end{cases}$$

Hence, we get for

$$\sum_{\alpha\in F_2^n}(-1)^{\langle\alpha,\beta\rangle}\prod_{a\in F_2^q} f_a^{a(\alpha,\dots)} = \prod_{i=1..n}\sum_{\xi\in F_2}(-1)^{\langle\beta_i,\xi\rangle} f_a^{a(\xi,\dots)}$$
$$= (f_0+f_1)^{0(\beta,\dots)}(f_0-f_1)^{1(\beta,\dots)}\cdots$$

We have proved

$$P_{C^\perp,C_2,\dots,C_q} = (\#C)^{-1}P_{C,C_2,\dots,C_q}(f_0+f_1, f_0-f_1,\cdots)$$

as desired. □

The above method yields the following equation:

$$P(C^\perp) = (\#C)^{-g}T(P(C))$$

with the matrix

$$T = \left((-1)^{\langle a,b\rangle}\right)_{a,b\in F_2^q}.$$

We have $T_g = (1+i/2)^g T$. The weight polynomial is homogeneous of degree n. Hence this equation may be rewritten in a more symmetric way as

$$T_g\left(\left(\frac{1}{\sqrt{2}}\right)^{g\,\cdot\,\dim(C)} P_g(C)\right) = (\varepsilon^{gn})\left(\frac{1}{\sqrt{2}}\right)^{g\,\cdot\,\dim(C^\perp)} P_g(C^\perp).$$

We call this formula MacWilliams equation.

The weight polynomial is homogeneous of degree divisible by 8 (self-dual doubly-even codes only exist in such length). Hence 3.1 may be reformulated as follows: The weight polynomial is invariant under the element

$$W = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & & & 0 & \\ 1 & -1 & & & & \\ & & 1 & 1 & & \cdots \\ & 0 & 1 & -1 & & \\ & & \vdots & & \ddots & \end{pmatrix}.$$

A self-dual code always contains the vector 1 ($1 * x = x = x * x$, hence $\langle x,1\rangle = \langle x,x\rangle = |x| = 0$). Moreover, the property of being a linear code may be expressed as

3.3. *The weight polynomial in genus g of a code which contains the vector* 1 *is always AGl(g)-invariant, where AGl(g) is considered as a subgroup of permutations in* $Gl(2^g,\mathbb{Z})$.

3.4. *The weight polynomial in genus g of a doubly-even code is always invariant under the action of* D_g, *where* D_g *is the abelian subgroup of* H_g *generated by the diagonal matrices* D_S.

We have proved:

Theorem 3.5. *For any (self-dual doubly-even) code the weight polynomial in genus g is invariant under the action of the group G_g, hence $P_g(C) \in CP_g$.*

We have the homomorphism

$$Th_g : B_g \longrightarrow \bigoplus_k [\Gamma_g^*(2,4), k]$$

given by evaluating the f_a as theta constants of second order. The restriction

$$Th_g : CP_g \longrightarrow \bigoplus_{4|k} [\Gamma_g, k]$$

is isomorphic for genus $g \leqslant 2$ and surjective for genus $g \leqslant 3$. For general genus, *Th* is only integral. Later we will see that the $Th(P_g(C))$ are just theta series of canonically associated lattices. The main statement of this paper is the following:

Theorem 3.6. *The ring CP_g is generated by $P_g(C)$ for (self-dual doubly-even) codes C.*

This theorem will be proved after some preparation. The theorem says that the MacWilliams identity is equivalent to self-duality. It is surprising to get the invariant ring in such an explicit way. The key point in our strategy will be the following: The group G_g is generated by a monomial group and the MacWilliams identity W. The ring of invariants is computed in two steps. The first step is to compute the invariants under the monomial group (see [36,37] or [33,34]). The second step is to apply the MacWilliams equation. The method to compute the invariant ring for the monomial group can be expressed in the framework of coding theory. By the surjectivity of the Φ-operator we may suppose that the genus is higher than the degree of an invariant polynomial which implies that the expression of the invariant polynomial as a linear combination of code polynomials of doubly-even codes is unique. Then the MacWilliams equation implies that the occurring codes have to be self-dual.

Remark 3.7. If the biweight polynomial of a linear code is invariant under the action of the group G_2, it is self-dual and doubly-even. (If there would be two codewords which are not orthogonal, they have an odd number of ones in common. Hence, in the biweight polynomial there would occur a monomial with an odd exponent in contrast to the group invariance.)

One may reformulate the conditions of (H_2, ε)-invariance for a polynomial

$$f = \sum a_{\alpha_0,\alpha_1,\alpha_2,\alpha_3} f_0^{\alpha_0} f_1^{\alpha_1} f_2^{\alpha_2} f_3^{\alpha_3}$$

as follows: The coefficient $a_{\alpha_0,\alpha_1,\alpha_2,\alpha_3}$ is different from zero only if

1. $8|\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3$,
2. $4|\alpha_0 + \alpha_1$,

3. $4|\alpha_0 + \alpha_2$,

4. $4|\alpha_0 + \alpha_3$

and moreover $W(f) = f$ holds.

Remark 3.8. We proved in [33] that H_2 is generated by (pseudo) reflections. The ring of invariants is generated by

$$P_8 = (8) + 14(4,4) + 168(2,2,2,2),$$

$$P_{12} = (12) - 33(8,4) + 330(4,4,4) + 792(6,2,2,2),$$

$$P_{20} = (14,2,2,2) - (12,4,4) - (10,6,2,2) + 2(8,8,4) + 13(8,4,4,4) - 14(6,6,6,2),$$

$$P_{24} = (24) + 759(16,8) + 2576(12,12) + 212\,520(12,4,4,4) + 340\,032(10,6,6,2) + 22\,770(8,8,8) + 1\,275\,120(8,8,4,4) + 40\,80\,384(6,6,6,6).$$

Here $P_8 = P_2(H_8)$ is the biweight polynomial of the Hamming code and P_{24} is the biweight polynomial of the Golay code G_{24}. Hence, the invariant ring of $G_2 = (H_2, \varepsilon)$ is generated by $P_8, P_{24}, P_{12}^2, P_{20}^2, P_{12}P_{20}$ which is the main result in [13]. One may rewrite this. The invariant ring is generated by biweight polynomials of self-dual doubly-even codes in length $8, 24, 24, 32, 40$. This may be proved directly or follows from 3.6.

The conditions of invariance for a polynomial in the f_a may be written as described in [33,34]. For the general theory we refer to Stanley [36,37]. All invariants are given as symmetrizations over $AGl(g)$ of admissible monomials (i.e. invariant under the group of diagonal matrices (D_g, ε)) and the additional condition of being W-invariant. We denote by

$$A = (a_0, \ldots, a_{2^g-1})$$

a tupel of exponents. It is *admissible* if

$$8 \Big| \sum_{b \in F_2^g} a_b = \deg(A)$$

and

$$4 \Big| \sum_{b \in F_2^g} a_b S[b] \text{ for all symmetric } g \times g\text{-matrices } S.$$

Here we regard b as a vector or a number via the binary number convention. For genus g there are $\binom{g+1}{2}$ conditions. Sometimes we replace the first condition by $4|\deg(A)$ if

we only regard invariants for H_g. We denote by

$$f_A = \sum_{\sigma \in AGl(g)/\mathrm{Stab}(A)} \prod_{b \in F_2^g} (f_b^{a_b})^\sigma$$

the symmetrization over $AGl(g)$. Then the invariant polynomials under (H_g, ε) are given as

$$f = \sum_{A \text{ admissible mod } AGl} c_A f_A$$

with the condition

$$W(f) = f.$$

Example 3.9. In genus three a tupel of exponents $A = (\alpha_0, \alpha_1, \ldots, \alpha_7)$ is admissible iff

1. $8 \left| \sum_{i=0..7} \alpha_i \right.$,
2. $4 | \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3$,
3. $4 | \alpha_0 + \alpha_2 + \alpha_4 + \alpha_6$,
4. $4 | \alpha_0 + \alpha_3 + \alpha_4 + \alpha_7$,
5. $2 | \alpha_6 + \alpha_7$,
6. $2 | \alpha_5 + \alpha_7$,
7. $2 | \alpha_3 + \alpha_7$,

We give two examples of weight polynomials in genus three:

$$P_3(H_8) = (8) + 14(4,4) + 168(2,2,2,2) + 1344(1,1,1,1,1,1,1,1),$$

$$\begin{aligned} P_3(H_8 \times H_8) &= (P_3(H_8))^2 \\ &= (16) + 28(12,4) + 198(8,8) + 420(8,4,4) \\ &\quad + 336(10,2,2,2) + 4704(6,6,2,2) \\ &\quad + 29\,400(4,4,4,4) + 2688(9,1,1,1,1,1,1,1) \\ &\quad + 336(8,0,0,0,2,2,2,2) + 4704(6,2,2,2,4,0,0,0) \\ &\quad + 37\,632(5,5,1,1,1,1,1,1) + 1176(4,4,4,0,4,0,0,0) \\ &\quad + 61\,152(4,4,0,0,2,2,2,2) + 451\,584(3,3,3,3,1,1,1,1) \\ &\quad + 2\,2014\,72(2,2,2,2,2,2,2,2), \end{aligned}$$

$$P_3(D_{16}^+) = (16) + 28(12,4) + 198(8,8) + 420(8,4,4)$$
$$+336(10,2,2,2) + 4704(6,6,2,2)$$
$$+29\,400(4,4,4,4) + 1680(8,0,0,0,2,2,2,2)$$
$$+3360(6,2,2,2,4,0,0,0) + 43\,008(5,5,1,1,1,1,1,1)$$
$$+2520(4,4,4,0,4,0,0,0) + 63\,840(4,4,0,0,2,2,2,2)$$
$$+430\,080(3,3,3,3,1,1,1,1) + 2\,298\,240(2,2,2,2,2,2,2,2).$$

(It is proved in [33] that the ring of modular forms (of level $\Gamma_3^*(2,4)$) is just defined by the equation $P_3(H_8 \times H_8) - P_3(D_{16}^+)$ which is mapped to zero under Φ, hence a "cusp" form for the polynomial ring. With the result in Section 4 we get $\Theta_{16} = \Theta_8^2$ in genus three where we denote with Θ_i the theta series of the unique even indecomposable lattice in dimension i for $i = 8, 16$. This computation gives a direct proof of a conjecture of Witt [40], proved independently by Igusa [15] and Kneser [21]. See also [17–19].)

Furthermore, weight polynomials of (self-dual doubly-even) codes have the obvious properties:

(3.10)

(1) $P_1(C)(0,1) = 1 = P_1(C)(1,0)$

(2) $P_1(C)(1,1) = 2^{\dim(C)} = \#(C)$

(3) $P_g(C) \in \mathbb{Z}[f_a \text{ with } a \in \boldsymbol{F}_2^g]^{(H_g,\varepsilon)}$ the coefficients of $P_g(C)$ are positive,

(4) $P_g(C_1 \times C_2) = P_g(C_1)P_g(C_2)$,

(5) $\Phi(P_{g+1}(C)) = P_g(C)$.

One may ask if one may get back the code from its code polynomials. For small genus the code polynomial does not contain enough information. But for a code of dimension d the weight polynomial $P_{d-1}(C)$ contains all the informations about the code. It contains a tupel of exponents for every configuration of $d-1$ codewords. Especially, one may find $d-1$ codewords, which together with the word 1 form a basis of the code. One has to choose some order in $\boldsymbol{F}_2^{d-1}$. We always use the standard one given by the binary number convention. The weight polynomial only depends on the isomorphism class of the code. This remark holds not only for self-dual doubly-even codes, but for all linear codes.

Example 3.11. The Hamming code H_8 is characterized by its weight polynomial

$$P_3(H_8) = (8) + 14(4,4) + 168(2,2,2,2) + 1344(1,1,1,1,1,1,1,1).$$

The last term (1, 1, 1, 1, 1, 1, 1, 1) gives back the code. We choose one times any element in $\boldsymbol{F}_2^3$ written as a vector and add a row for the codeword 1 and get the matrix

$$\begin{pmatrix} 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 1&1&1&1&1&1&1&1 \end{pmatrix}$$

which is a generating matrix for H_8. The monomial (1, 1, 1, 1, 1, 1, 1, 1) is an admissible monomial of maximal genus in the obvious sense.

We have proved in [35] the surjectivity of the Φ-operator. Hence, it is no restriction for an invariant polynomial in CP_g to suppose that the genus is higher than the degree. This will be used in the proof of Theorem 3.6.

The surjectivity of the Φ-operator may be used to consider invariant polynomials as living in arbitrary high genus, hence to regard the graded ring

$$CP_\infty = \varprojlim_g CP_g.$$

For any degree l it is given by code polynomials of self-dual doubly-even codes of length l.

We define

$$P_\infty(C) = P_g(C) \quad \text{for } g \geqslant \dim(C) - 1$$

as an element in CP_∞. For arbitrary codes containing 1 one may take the same definition and regards $P_\infty(C)$ as an element in

$$\varprojlim_g B_g^{(AGl(g))}.$$

From these remarks one gets an algorithm for computing all codes of a certain length l. One computes for some $g \geqslant l/2 - 1$ the invariants in the vector space

$$(B_g)_{(\deg = l)}$$

and the codes correspond to monomials of maximal genus modulo AGl. (More precisely one first determines the admissible monomials of maximal genus (see Section 5) and takes in any AGl-orbit a representative.)

Example 3.12. (Biweight polynomials in length 24). One may compute the space of polynomials which fulfil the conditions 3.1, 3.5 and 3.10. in degree 24 and genus 2. One gets a diophantine system of equations with the following solution. The polynomials

are given by

$$(24)+3A(20,4)+3(253-4A)(16,8)+2(1288+9A)(12,12)$$
$$+3A(2A+1)(16,4,4)+6A(127-A)+12(19A^2-908A+17710)(12,4,4,4)$$
$$+18(6A^2-102A+1265)(8,8,8)+18(6A^2-267A+70\,840)(8,8,4,4)$$
$$+3A(A-2)(18,2,2,2)+36(42-A)(14,6,2,2)+66A(A+94)(10,10,2,2)$$
$$-12(13A^2+582A-28\,336)(10,6,6,2)-24(A^2-3746A-170\,016)(6,6,6,6)$$

as a solution of this problem together with the conditions

$$0\leqslant A\leqslant 29 \quad \text{and} \quad A\neq 1.$$

But only the numbers $A\in\{0,2,4,6,8,10,14,22\}$ correspond to self-dual doubly-even codes.

Remark 3.13. One may as well study the group for self-dual codes which is generated by $AGl(g)$ and the element W. If one denotes (as in [34]) the permutation $P=(1,2)(3,4)\cdots$ then $WPW=E^2$. Hence a self-dual code is always even. In genus one it is a group generated by reflections of order 16, the ring of invariants is generated by $P_1([2,1,2])=(2)=f_0^2+f_1^2$ and $P_1(H_8)=(8)+14(4,4)$. We denote by $[2,1,2]$ the (unique) code generated by 0 and 1. For higher genus we regard the permutation $Q=(1,2)(5,6)\cdots$ which is the image of $(1,2)\in H_2$ under a diagonal embedding of the group H_2 and the equation $WQW=\mathrm{diag}(1,-1,1,1,\ldots)$. The equation proves that all the elements E_{ij} are in the subgroup generated by $AGl(g)$ and W.

Remark 3.14. Last, but not least we consider the genus one case. The group G_1 is a group generated by (pseudo) reflections of order 192 and the ring of invariants is given by

$$CP_1=\mathbb{C}[(8)+14(4,4),(24)+759(16,8)+2576(12,12)]=\mathbb{C}[P_1(H_8),P_1(C_{24})],$$

where C_{24} is any code of length 24 different from H_8^3 and $H_8\times D_{16}^+$. For example, one may take the Golay code as above or D_{24}^+ with

$$P_1(D_{24}^+)=(24)+66(20,4)+495(16,8)+2972(12,12)$$

(the constant A in the list in 3.12 is given by $A=22$). This is a result of Gleason [10]. The corresponding result for modular forms is classical. A proof follows from the computation of the ring of invariants for the group H_1 given in [33, p. 68.]

Remark 3.15. The diagonal code in H_g.

We want to state just as a curiosity that there is a code sitting inside the group H_g. One may take the imaginary part of the diagonal matrices in H_g and get a $[2^g,g+1,2^{g-1}]$-code with automorphism group $AGl(g)$. This diagonal code is for small genus neither self-dual nor doubly-even, but for genus $g\geqslant 3$ it becomes double-even and

weakly self-dual (i.e. $1 \in C \subset C^{\perp}$). For genus one it is the $[2,2,1]$-code with S_2 as automorphism group, for genus two it is the $[4,3,2]$-code (sum zero code) with automorphism group S_4, for genus three it is the Hamming code, for genus four it is the $[16,5,8]$-code RM (usually called Reed–Muller-code) with $Aut(RM) = AGl(4)$ of order 322,560.

4. Codes and lattices

There are many ways to associate a lattice to a code. We refer to [4] for much interesting material. There are described the constructions A,B,C,D. For our purpose the construction A is the most important.

Denote by $\psi : \mathbb{Z}^n \longrightarrow \boldsymbol{F}_2^n$ the canonical morphism, then we get with

$$\Lambda(C) = \frac{1}{\sqrt{2}}(\psi^{-1}(C)) \subset \mathbb{R}^n$$

the construction A. For a self-dual doubly-even code C of dimension d we get an unimodular even lattice of dimension $2d = \text{length}(C)$, which is easily checked. If the generator matrix of the code is denoted by $(1, M)$, we get a generator matrix of the lattice by first filling up $(1, M)$ with some rows with exactly one entry 2 to get a regular quadratic matrix

$$T = \begin{pmatrix} 1 & M \\ 0 & 2 \end{pmatrix}$$

and after this $S = (1/2)TT^{\mathrm{t}}$ gives an even symmetric matrix. (We identify the quadratic form which belongs to S and the lattice Λ.)

It is well known that any (positive-definite symmetric) $S \in Sl(d, \mathbb{Z})$ may be written as $S = 2^{-k}MM^{\mathrm{t}}$ for some $M \in Mat_d(\mathbb{Z})$. Hence, one may define

$$h(S) = \min\{k \mid \text{there exists } M \in Mat_d(\mathbb{Z}) \text{ with } S = 2^{-k}MM^{\mathrm{t}}\}$$

and self-dual doubly-even codes correspond to even unimodular lattices with $h(S) \leqslant 1$. Codes are also in another sense the simplest lattices.

As usual we call the elements of (euclidian) length 2 roots and the set of all roots root system. Self-dual doubly-even codes correspond (bijectively) to even lattices with a root system containing nA_1 (the root system contains an orthogonal basis of $\mathbb{R}^n$). Hence, self-dual doubly-even codes are the easiest lattices with respect to the root system, see [22].

There are many more lattices than codes. In dimension 8 the (unique) even lattice comes from the Hamming code $H_8 = D_8^+$, in dimension 16 the two even lattices come from the two codes of length 16 (i.e. H_8^2 and D_{16}^+). In dimension 24 there are 24 even lattices (Niemeier), but only 9 coming from codes. In dimension 32 there exist 85 even lattices coming from codes, but more than 80 millions even lattices. In length 40 there are already more than 17 000 self-dual doubly-even codes.

The theta series in genus g for a lattice S or Λ of dimension d is given for $\tau \in \mathbb{H}_g$ by

$$\Theta_S(\tau) = \sum_{G \in M_{d,g}(\mathbb{Z})} \exp(\pi i Tr(G^t S G \tau)).$$

By a straightforward computation one gets

Proposition 4.1.

$$\Theta_{\Lambda(C)}(\tau) = Th(P_g(C)).$$

Remark 4.2. Proposition 4.1 may be regarded as a special case of formula $R_{ch}^{T,Q}$ in [27, p. 219] for $Q = 2$ and $z = 0 = A = B$ and A' and B' replaced by A and B. For $S = 2T^tT$ with $T \in Mat_d(\mathbb{Q})$ we have

$$\Theta_S(\tau) = k^{-1} \sum_{A \in K_1, B \in K_2} \theta \begin{bmatrix} A \\ B \end{bmatrix} (2\tau)$$

where $k = \#K_2$ and

$$K_1 = Mat_{g,d}(\mathbb{Z})T^t / Mat_{g,d}(\mathbb{Z})T^t \cap Mat_{g,d}(\mathbb{Z})$$

and

$$K_2 = Mat_{g,d}(\mathbb{Z})T^{-1} / Mat_{g,d}(\mathbb{Z})T^{-1} \cap Mat_{g,d}(\mathbb{Z}).$$

For a matrix as above coming from a code $S = (1/2)TT^t = 2(\frac{1}{2}T)(\frac{1}{2}T^t)$ with

$$T = \begin{pmatrix} 1 & M \\ 0 & 2 \end{pmatrix}$$

we get for

$$(\tfrac{1}{2}T)^{-1} = \begin{pmatrix} 2 & -M \\ 0 & 1 \end{pmatrix} \in Mat_{g,d}(\mathbb{Z}),$$

hence $K_2 = 0$ and $k = 1$ and for the product of theta constants we get $\theta\left[\begin{smallmatrix} A \\ 0 \end{smallmatrix}\right](2\tau)$; hence the product of theta constants of second order as desired. This remark arose out of a discussion with R. Salvati Manni in Rome.

It is well known that even unimodular lattices only exist for dimension d a multiple of 8. The theta series is then a modular form of weight $d/2$. The cokernel of the inclusion

$$\mathbb{C}[\Theta_\Lambda \text{ with } \Lambda \text{ an even unimodular lattice}] \subset \bigoplus_{4|k} [\Gamma_g, k]$$

is zero for $2k < g$ and $k > 2g$, see [1]. For genus one, two and three the inclusion is an isomorphism and one may reformulate 3.6 (or 3.8 and 3.14) as follows.

Theorem 4.3. *The ring* $\bigoplus_{4|k}[\Gamma_g,k]$ *is for* $g\leqslant 3$ *generated by theta series of even unimodular lattices coming from self-dual doubly-even codes. For arbitrary genus,* $\bigoplus_{4|k}[\Gamma_g,k]$ *is the normalization of* $\mathbb{C}[\Theta_{\Lambda(C)}]$ *for self-dual doubly-even codes C in its field of fractions. Moreover, the normalization map* $Th : \mathcal{A}_g \to Proj(CP_g)$ *is a homeomorphism onto its image.*

The ring of theta series of lattices is just the ring of stable modular forms [7]. A modular form $f \in [\Gamma_g,k]$ is called *stable*, if for any number i there exists a modular form $F \in [\Gamma_{g+i},k]$ such that $\Phi^i(F) = f$. The image $Th(CP_g)$ is a subring in the ring of stable modular forms. For $2k < g$ and $4|s$ the Φ-operator is an isomorphism (singular modular forms). This corresponds to the fact that a code of dimension d is determined by its weight polynomial in genus $d-1$.

5. Mean polynomials and the Proof of Theorem 3.6

We considered the weight polynomials of self-dual doubly-even codes and proved the invariance under G_g. Hence, also the polynomial

$$M_n^{(g)} = \frac{1}{\#\{\text{ codes in length } n\}} \sum_{\text{codes } C} P_g(C)$$

is G_g-invariant and called *mean polynomial* in length $n = 2d$ and genus g ($d = \dim(C)$).

We fix the notation

$$C(s,d) = \begin{cases} 1 & \text{if } s = d \\ (2^0+1)\cdots(2^{d-s-1}+1) & \text{if } s < d \end{cases}$$

for the number of self-dual doubly-even codes containing a doubly-even code containing 1 of dimension s and

$$\mathcal{M}_d = \{\text{ self-dual doubly-even codes in length } 2d\}$$

with cardinality $C(1,d) = 2\cdot 3\cdots(2^{d-3}+1)\cdot(2^{d-2}+1)$. To state the result we fix

$$\binom{n}{a_1;a_2;\ldots;a_l} = \frac{n!}{a_1!\cdot a_2!\cdots a_l!}$$

and define the genus $g(A)$ of an admissible tupel of exponents

$$A = (a_0,\ldots,a_{2^g-1})$$

for H_g to be the smallest g such that the monomial is admissible (One has to regard admissible monomials modulo the AGl-action). To avoid exceptions in the following formulae, we use the (formal) genus zero case, i.e. $B_0 = \mathbb{C}[f_0]$, $CP_0 = \mathbb{C}[f_0^8] = \mathbb{C}[(8)]$,

$H_0 = \langle i \rangle = H_{0,4} = N_0$ (is the cyclic group of order four), $G_0 = \langle \varepsilon \rangle$ (cyclic of order eight), $\Phi(f_0) = f_0$, $\Phi(f_1) = 0, \ldots$

Example 5.1.

$$g((8)) = 0,$$
$$g((2,2,2,2)) = 2,$$
$$g((2,2,0,0,2,2,0,0)) = 2,$$
$$g((8,0,0,0,2,2,2,2)) = 3.$$

We recall the notation

$$f_A = \sum_{\sigma \in AGl(g)/\mathrm{Stab}(A)} \prod_{b \in F_2^g} (f_b^{a_b})^\sigma$$

for the symmetrization of an admissible monomial.

Theorem 5.2. *The mean polynomial can be computed as*

$$\begin{aligned} M_{2d}^{(g)} &= \frac{1}{\#\mathcal{M}_d} \sum_{C \in \mathcal{M}_d} P_g(C) \\ &= \sum_{\substack{A \text{ admissible} \\ (\mathrm{mod} AGl), \deg(A)=2d}} \frac{C(1+g(A),d)}{\#\mathcal{M}_d} \binom{2d}{A} f_A \\ &= (2d) + \sum_{0<x<2d, 4|x} \binom{2d}{x} (2d-x,x) \frac{1}{1+2^{d-2}} \\ &\quad + \sum_{r=2}^{g} \sum_{\substack{A \text{ admissible} \\ (\mathrm{mod} AGl),\, g(A)=r,\, \deg(A)=2d}} \binom{2d}{A} f_A \frac{1}{(1+2^{d-2}) \cdots (1+2^{d-1-r})} \end{aligned}$$

Example 5.3. Let $n = 8$ and $g = 3$. We get

$$\begin{aligned} M_8^{(3)} &= (8) + \binom{8}{4} (4,4) \frac{1}{1+2^2} + \binom{8}{2;2;2;2} (2,2,2,2) \frac{1}{(1+2^2)(1+2)} \\ &\quad + \binom{8}{1;1;1;1;1;1;1;1} (1,1,1,1,1,1,1,1) \frac{1}{(1+2^2)(1+2)(1+1)} \\ &= (8) + 14(4,4) + 168(2,2,2,2) + 1344(1,1,1,1,1,1,1,1) \\ &= P_3(H_8) \end{aligned}$$

in accordance with the fact that H_8 is the unique self-dual doubly-even code in length 8.

For the proof of the theorem we introduce the following notations. We call

$$\begin{aligned}\alpha &= \text{ a tupel of } g \text{ elements } \alpha_1,\dots,\alpha_g \in \boldsymbol{F}_2^{2d},\\ C(\alpha) &= \text{ the code generated by 1 and } \alpha,\\ s(\alpha) &= \dim(C(\alpha)).\end{aligned}$$

Then we get the formula

$$\#\{C \in \mathcal{M}_d \text{ with } \alpha \subset C\} = \begin{cases} C(s(\alpha),d) & \text{if } C(\alpha) \text{ doubly-even}\\ 0 & \text{else.}\end{cases}$$

We use the correspondence

$$\begin{array}{ccc}\alpha & & A(\alpha) = (a_0,\dots,a_{2^g-1})\\ \text{a tupel of codewords} & \longleftrightarrow & \text{an admissible tupel of exponents}\end{array}$$

which is given by

$$f^{A(\alpha)} = \prod_{a\in \boldsymbol{F}_2^g} f_a^{a(\alpha)}$$

(note the difference between f^A which is a monomial and f_A which is the symmetrization of f^A).

Now we make the following three observations:

$$C(\alpha) \text{ doubly-even} \iff f^{A(\alpha)} = \prod_{a\in \boldsymbol{F}_2^g} f_a^{a(\alpha)} \text{ is an admissible monomial}$$

and

$$\dim(C(\alpha)) = s(\alpha) = 1 + g(A(\alpha))$$

and

$$\#\mathrm{Stab}(A) = A! = a_0!\cdots a_{2^g-1}!$$

for an admissible tupel of exponents (which corresponds to changing the order of coordinates). The permutations of the rows in the $g \times 2d$-matrix α correspond to the action of S_{2d}.

Hence,

$$\begin{aligned}M_{2d}^{(g)} &= \frac{1}{\#\mathcal{M}_d}\sum_{C\in\mathcal{M}_d} P_g(C)\\ &= \frac{1}{\#\mathcal{M}_d}\sum_{C\in\mathcal{M}_d}\sum_{\alpha\in C} f^{A(\alpha)}\\ &= \frac{1}{\#\mathcal{M}_d}\sum_{\alpha}\#\{C\in\mathcal{M}_d \text{ with } \alpha\subset C\} f^{A(\alpha)}\end{aligned}$$

and with the above observations we get the formula of Theorem 5.2.

One may use the mean polynomials to write down explicitly modular forms without knowing any code. The numerical problems to compute higher weight polynomials of a given code are relatively big as one may imagine from the examples.

For the proof of Theorem 3.6 we define

$$\mathcal{W}_d = \{\text{doubly-even codes containing 1 in length } 2d\}$$

and

$$\mathcal{W} = \uplus_d \mathcal{W}_d$$

for the set of doubly-even codes containing 1. The correspondence above may be reformulated as

$$B_g^{(H_{g,4})} = \mathbb{C}[P_g(D) \text{ with } D \in \mathcal{W}] = \mathbb{C}[f_A \text{ with } A \textit{ admissible}].$$

With the same argument one has

$$B_g^{(AGl(g))} = \mathbb{C}[P_g(D) \text{ with } D \text{ a code containing } 1].$$

Example 5.4.

$$\begin{aligned} P_\infty(Rep_n) &= (n), \\ P_\infty(Rep_4) &= P_\infty(D_4) = (4), \\ P_\infty(D_4 \times D_4) &= (4)^2 = (8) + 2(4,4), \\ P_\infty(D_8) &= (8) + 6(4,4) + 24(2,2,2,2), \\ 1344(1,1,1,1,1,1,1,1) &= P_\infty(H_8) - 7P_\infty(D_8) + 14P_\infty(D_4 \times D_4) - 15P_\infty(Rep_8). \end{aligned}$$

One may describe the correspondence between doubly-even codes containing 1 and admissible monomials more explicitly (like in 3.11).

$$\begin{array}{ccc} A = (a_0, \ldots, a_{2^g-1}) & & D(A) \\ \text{an admissible tupel of exponents} & \longleftrightarrow & \text{a doubly-even code containing 1} \end{array}$$

which is given by

$$D(A) = \begin{pmatrix} \overbrace{0, \cdots, 0}^{a_0} & \cdots & \overbrace{2^g - 1, \cdots, 2^g - 1}^{a_{2^g-1}} \\ 1 & \cdots & 1 \end{pmatrix}.$$

This should be read as follows. The number i as binary number with g digits is a_i-times written as a vector in $\boldsymbol{F}_2^g$ and together with a row consisting of ones one gets a $(g+1) \times (deg(A))$-matrix $D(A)$. Then

$$P_g(D(A)) = \frac{\#Aut(D(A))}{A!} f_A + \text{ terms of lower genus}$$

Proof of Theorem 3.6. Let

$$f = \sum_i d_i P_g(D_i)$$

be a homogeneous polynomial of degree $2d$ with $D_i \in \mathcal{W}_d$ and $4|d$. Then the MacWilliams equation yields

$$T_g(f) = T_g\left(\sum_i d_i P_g(D_i)\right) = \sum_i d_i \left(\frac{1}{\sqrt{2}}\right)^{g(\dim(D_i^\perp)-\dim(D_i))} P_g(D_i^\perp)$$

for arbitrary genus g. The $P_g(D_i^\perp)$ are uniquely determined by terms of maximal genus for genus $g \geqslant \dim(D_i^\perp) - 1$. Hence, for a H_g-invariant polynomial f for $g \gg 0$ in the above sum only self-dual codes occur. This ends the proof of Theorem 3.6. □

The analogue of Theorem 4.3 for the Hecke group $\Gamma_{g,0}$ is the following:

Theorem 5.5. *The rings* $\bigoplus_{2|k}[\Gamma_{g,0}(2),k]$ *are for* $g \leqslant 3$ *generated by theta series of even lattices coming from doubly-even codes containing 1. For arbitrary genus* $\bigoplus_{2|k}[\Gamma_{g,0}(2),k]$ *is the normalization of* $\mathbb{C}[\Theta_{\Lambda(C)}]$ *for doubly-even codes C containing 1 in its field of fractions. Moreover, the normalization map Th* : $\mathcal{A}_{g,0}(2) \to Proj(\mathbb{C}[P_g(C)])$ *(for doubly-even codes C containing 1) is a homeomorphism onto its image.*

6. Liftings

In the same way as in the definition of Eisenstein liftings for modular forms one may define a canonical map by symmetrization over the corresponding finite group. In this case there is of course no problem with convergency of a certain series, but does these maps define liftings?

We denote for $r \leqslant s$ by

$$i_{r,s} : B_r \longrightarrow B_s$$

the inclusion given by $f_a \mapsto f_a$. We regard a as a binary number with r or with s digits.

Then the map $L_{r,s}$ is defined by

$$L_{r,s}(f) = \frac{1}{\#H_s} \sum_{\sigma \in H_s} \sigma(i_{r,s}(f)).$$

For an admissible tupel of exponents

$$A = (a_0, \ldots, a_{2^r-1})$$

for H_r we denote by

$$c_{r,s}(A) = \frac{\#(H_r/\mathrm{Stab}(A))}{\#(H_s/\mathrm{Stab}(i_{r,s}(A)))}$$

the ratio of the numbers of terms after symmetrization over the corresponding AGl. Then we get the following formula:

Proposition. For an admissible monomial f^A for H_r it holds

$$L_{r,s}(f_A) = \frac{c_{r,s}(A)}{[H_s : H_{s,4}]} \sum_{\sigma \in H_s/H_{s,4}} \sigma(f_A).$$

Proof. For the proof we split the symmetrization over H_s into two steps. The first step is the symmetrization over $H_{s,4}$ which is given by taking the same admissible monomial. The number of terms increases and is given by the number $c_{r,s}$. The second step is the symmetrization over a set of representatives for $H_s/H_{s,4}$. Hence we get the above formula. □

It holds that

$$L_{r,s} \circ L_{t,r} = L_{t,s}.$$

To give some examples we always use the decomposition of H_s as described in [34]. There an explicit procedure to compute a set of representatives is given.

Example. A special case is $r = s = 2$:

$$\begin{aligned}
L_{2,2}((12)) &= \frac{7}{128} P_{12}, \\
L_{2,2}((8,4)) &= \frac{-7}{640} P_{12}, \\
L_{2,2}((6,2,2,2)) &= \frac{1}{1920} P_{12}, \\
L_{2,2}((4,4,4)) &= \frac{1}{1920} P_{12}, \\
L_{2,2}(P_{12}) &= P_{12}.
\end{aligned}$$

One may conjecture that

$$L_{0,g}((2d)) = (\mathrm{const}) M_{2d}^{(g)}$$

for $4|d$. It follows from Theorem 3.6 that

$$L_{r,s}(P_r(C)) = \sum_{C_i} \mathrm{const}_i P_s(C_i)$$

for some constants which depend on the self-dual doubly-even codes C and C_i. Conjecturely only codes C_i with $P_r(C_i) = P_r(C)$ occur. It would follow from this conjecture that for big genus r the map $L_{r,s}$ is indeed a lifting for weight polynomials.

There is another map $K_{r,s}$ defined by taking the same admissible monomial

$$K_{r,s}(f_A) = f_{(i_{r,s}(A))}.$$

We always have

$$\Phi^{s-r}(K_{r,s}(f)) = f;$$

hence we get a lifting, but only for

$$r \geqslant \tfrac{1}{2}\deg(f) - 1$$

it follows from Theorem 3.6 that we get an invariant polynomial in CP_s for $f \in CP_r$ (any invariant polynomial is a linear combination of $P_\infty(C)$ for codes C and $K_{r,s}(P_r(C)) = P_s(C) = P_\infty(C)$ for $r \geqslant \dim(C) - 1$).

7. Self-dual codes

The method of the previous sections also work for self-dual codes. We only want to state the results. The relevant group is generated by AGl and W. In the notations of Lemma 2.1 we have the exact sequence

$$0 \to \langle D_S^2, P_S\rangle \longrightarrow \langle AGl(g), W\rangle \longrightarrow O^+(2g, \boldsymbol{F}_2) \to 0.$$

The group $\langle D_S^2, P_S\rangle$ has order 2^{2g+1} and is an extraspecial 2-group of positive type (i.e. may be written as central product of g Dieder-groups D_8). The factor group $\langle D_S^2, P_S\rangle/\langle -1\rangle = \boldsymbol{F}_2^{2g}$ is an elementary abelian group, and the right homomorphism is given by the conjugation of $\langle AGl, W\rangle$ on this $\boldsymbol{F}_2$-vector space. The MacWilliams identity W preserves the quadratic form (and the symplectic form), but for the factor group we only get the orthogonal group. We have for the index $[Sp(2g, \boldsymbol{F}_2) : O^+(2g, \boldsymbol{F}_2)] = 2^{g-1}(2^g + 1)$ (which is the number of even theta characteristics), hence we get for the group order

$$\#(AGl(g), W) = 2^{g^2+g+2}(2^g - 1)(4^{g-1} - 1)\cdots 3 \quad \text{for } g \geqslant 2$$

and for genus one 16 (see 3.13).

By using the Veronese map (as in [35]) one gets the surjectivity of the Siegel Φ-operator

$$\Phi : B_g^{(AGl(g),W)} \longrightarrow B_{g-1}^{(AGl(g-1),W)}$$

and with the same argument as in Section 5 we get:

Theorem 7.1. *The ring of invariants $B_g^{(AGl(g),W)}$ is generated by $P_g(C)$ for self-dual codes C.*

The admissible monomials correspond to even codes containing 1. The lattices $\Lambda(C)$ are unimodular lattices (but in general not even). The morphism Th maps

$$Th : B_g^{(AGl(g),W)} \longrightarrow \mathbb{C}[\Theta_\Lambda \text{ with } \Lambda \text{ a unimodular lattice }].$$

If the degree is divisible by 8 the image $Th(f)$ is an element in $\oplus_{4|s}[\Gamma_g(1,2),s]$, where $\Gamma_g(1,2)$ is the theta group defined for a symplectic matrix

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

by the condition

$${}^tAC \text{ and } {}^tBD \text{ have even diagonal entries.}$$

In the notation of Section 2 we have

$$\phi(\Gamma_g(1,2)) = (N_g, AGl(g), M_i)/(\pm 1).$$

The matrices M_1 and W differ by an eighth root of unity. Hence, for this level the relation between codes and modular forms is smooth only for the 4-ring.

The computation of the invariant ring for genus one is started in 3.13. The group

$$M_1 = \left(\frac{1+i}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right)$$

is generated by reflections of order 32 and the invariant ring is

$$\bigoplus_s [\Gamma_1(1,2),s] = \mathbb{C}[(8) + 14(4,4), (4) - 6(2,2)].$$

For genus two, $(AGl(2), W) = (S_4, \mathrm{diag}(\pm 1, \pm 1, \pm 1, \pm 1), W)$ is not generated by reflections, but there is a subgroup of index two generated by reflections. Let

$$T = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

then $(S_4, \mathrm{diag}(\pm 1, \pm 1, \pm 1, \pm 1), T)$ is a group generated by reflections (obviously) of order 1152 and the invariant ring is generated by

$$P_2 = (2),$$

$$P_6 = (6) - 5(4,2) + 30(2,2,2),$$

$$P_8 = P_2(H_8)$$

$$= (8) + 14(4,4) + 168(2,2,2,2),$$

$$P_{12} = (12) - 33(8,4) + 330(4,4,4) + 792(6,2,2,2).$$

(Huffman uses instead of P_{12} a constant multiple of the polynomial

$$(12) - 6(10,2) + 15(8,4) - 84(6,6) - 390(4,4,4) + 84(6,4,2) + 1260(4,4,2,2) - 936(6,2,2,2) + 18(8,2,2).$$

There is of course some freedom in choosing invariants in degree 6,8 and 12.) One may check that

$$W(P_2) = P_2,$$
$$W(P_6) = -P_6,$$
$$W(P_8) = P_8,$$
$$W(P_{12}) = -P_{12}.$$

Hence,

$$B_2^{(AGl(2),W)} = \mathbb{C}[P_2, P_8, P_6^2, P_6P_{12}, P_{12}^2]$$

is a hypersurface of degree 36. This result is already contained in [13] and cited there from a joint paper of MacWilliams, Mallows and Sloane. One may rewrite this. The invariant ring is generated by biweight polynomials of self-dual codes in length 2,8,12,18 and 24. The code in length 2 is the unique Rep_2-code, the code in length 8 may be chosen as the Hamming-code and the other codes are easy to choose.

For computing modular forms one has to deal with the group of order 4608,

$$\big(M_1, S_4, \mathrm{diag}(\pm 1, \pm 1, \pm 1, \pm 1)\big).$$

The group $(S_4, \mathrm{diag}(\pm 1, \pm 1, \pm 1, \pm 1), T)$ is again a subgroup generated by reflections and one may check that

$$M_1(P_2) = iP_2,$$
$$M_1(P_6) = iP_6,$$
$$M_1(P_8) = P_8,$$
$$M_1(P_{12}) = P_{12}.$$

Hence,

$$\bigoplus_{2|k} [\Gamma_2(1,2), k] = \mathbb{C}[P_2^4, P_2^3P_6, P_2^2P_6^2, P_2P_6^3, P_6^4, P_8, P_{12}]$$

and the Poincaré-series is given by

$$\Phi_{\Gamma_2(1,2)_{(2)}}(\lambda) = \frac{1 + \lambda^6 + \lambda^8 + \lambda^{10}}{(1-\lambda^4)^2(1-\lambda^6)(1-\lambda^{12})}$$

which is easy to check (remember that the weight is half of the degree).

For the ring $\bigoplus[\Gamma_2^*(2,4),k] = \mathbb{C}[f_a f_b][\Theta]$ the action of the group H_2 on Θ is given by the determinant. Hence, with the help of Lemma 4.2 in [33] one can compute the Poincaré-series as

$$\Phi_{\Gamma_2(1,2)}(\lambda) = \frac{1+\lambda^6+\lambda^8+\lambda^{10}+\lambda^{19}+\lambda^{21}+\lambda^{23}+\lambda^{29}}{(1-\lambda^4)^2(1-\lambda^6)(1-\lambda^{12})}$$

(in accordance with [14, p. 105]) and the full ring of invariants conjecturely as

$$\bigoplus[\Gamma_2(1,2),k] = \mathbb{C}[P_2^4, P_2^3P_6, P_2^2P_6^2, P_2P_6^3, P_6^4, P_8, P_{12}, P_{28}\Theta, P_{32}\Theta, P_{36}\Theta]$$

with P_i a certain polynomial of degree i. (The problem with polynomials in theta constants, which are unstable as modular forms, only occur for even genus and odd weight and for even, but not doubly-even weight in higher genus.)

For higher genus the group $(AGl(g), W)$ is free of reflections and moreover a subgroup of $SO(2^g, \mathbb{Z}[1/\sqrt{2}])$. The decomposition of Bruhat type [34] may be rewritten to make explicit computations for higher genus.

The analogue of Theorem 4.3 is the following:

Theorem 7.2. *The rings $\bigoplus_{4|k}[\Gamma_g(1,2),k]$ are for $g \leqslant 3$ generated by theta series of unimodular lattices coming from self-dual codes. For arbitrary genus, $\bigoplus_{4|k}[\Gamma_g(1,2),k]$ is the normalization of $\mathbb{C}[\Theta_{\Lambda(C)}]$ for self-dual codes C (of length divisible by 8) in its field of fractions. Moreover, the normalization map $Th : \mathcal{A}_g(1,2) \to Proj(\mathbb{C}[P_g(C)]$ (for self-dual codes C) is a homeomorphism onto its image.*

References

[1] S. Böcherer, Über die Fourier–Jacobi–Entwicklung Siegelscher Eisensteinreihen, Math. Z. 183 (1983) 21–46.

[2] M. Broué and M. Enguehard, Polynômes des poids de certains codes et fonctions thêta de certain réseaux, Ann. Scient. Éc. Norm. Sup., 4^e série t.5 (1972) 157–181.

[3] J.H. Conway and V. Pless, On the enumeration of self-dual codes, J. Combin. Theory A28 (1980) 26–53.

[4] J.H. Conway and N.J.A. Sloane, Sphere Packings, Lattices and Groups (Springer, Berlin, 1988).

[5] L. Dornhoff, Group Representation Theory A (Marcel Dekker, New York, 1971).

[6] J.S. Frame, Some characters of orthogonal groups over the field of two elements, in: Proc. 2nd Internat. Conf. on the Theory of Groups, Lecture Notes in Math., Vol. 372 (Springer, Berlin, 1974) 298–314.

[7] E. Freitag, Stabile Modulformen., Math. Ann. 230 (1977) 197–211.

[8] E. Freitag, Siegelsche Modulfunktionen, Grundlehren der Math. Wissenschaften, Vol. 254 (Springer, Berlin, Heidelberg, New York, 1983)

[9] E. Freitag, Singular Modular Forms and Theta Relations. (Lecture Notes in Math., Vol. 1487) (Springer, New York, 1991).

[10] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities. in: Actes Congrès Intern. des Mathématiciens (Nice 1970), Tome 3 (Gauthier-Villars, Paris, 1971) 211–215.

[11] R.L. Griess, Jr., Automorphisms of extra special groups and nonvanishing degree 2 cohomology, Pacific J. Math. 48, (1973) 403–422.

[12] R. Hartshorne, Algebraic Geometry, GTM 52 (Springer, New York, 1977).

[13] W.C. Huffmann, The biweight enumerator of selforthogonal binary codes, Discrete Math. 26 (1979) 129–143.

[14] J. Igusa, On Siegel modular forms of genus two (2), Am. J. Math. 86 (1964) 392–412.

[15] J. Igusa, Modular forms and projective invariants, Am. J. Math. 89 (1967) 817–855.
[16] J. Igusa, Theta functions Grundlehren der Math. Wissenschaften, Vol. 194 (Springer, Berlin, 1972).
[17] J. Igusa, Schottky's invariant and quadratic forms, in: E.B.Christoffel, The Influence of his Work on Math. and Physical Sci. (Butzer/Fehér) (Birkhäuser, Basel, 1981) 352–362.
[18] J. Igusa, On the irreducibility of Schottky's divisor, J. Fac. Sci. Univ. Tokyo 28 (1982) 531–545.
[19] J. Igusa, Problems on theta functions, in: Proc. Symp. in Pure Math., Vol. 49, Part 2 (Theta Functions Bowdoin 1987) (1989) 101–110.
[20] W. Jones and B. Parshall, On the 1-cohomology of finite groups of Lie type, in: W.R. Scott and F. Gross, eds., Proc. Conf. on Finite groups, Utah. 1975 (Academic Press, New York, 1977) 313–328.
[21] M. Kneser, Lineare Relationen zwischen Darstellungsanzahlen quadratischer Formen, Math. Ann. 168 (1967) 31–39.
[22] H. Koch, Unimodular lattices and self-dual codes, Proc. Internat. Congress of Math. Berkeley (1986).
[23] H. Koch, On self-dual, doubly even codes of length 32, J. Combin. Theroy A51 (1989) 63–76.
[24] H. Koch and B.B. Venkov, Über gerade unimodulare Gitter der Dimension 32, Preprint MPI Bonn, 1989.
[25] A. Krazer, Lehrbuch der Thetafunktionen (Teubner, Leipzig, 1903).
[26] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, Good self-dual codes exist, Discrete Math. 3 (1972) 153–162.
[27] D. Mumford, Tata Lectures on Theta 1–3, Progress in Math., Vol. 28,43,97 (Birkhäuser, Boston, 1983/84/91).
[28] J. Milnor and D. Husemoller, Symmetric bilinear forms, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73 (Springer, Berlin, 1973).
[29] V. Pless, A classification of self-orthogonal codes over GF(2), Discrete Math. 3 (1972) 209–246.
[30] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, J. Combin. Theory A18 (1975) 313–335.
[31] H.E. Rauch and H.M. Farkas, Theta Functions with Applications to Riemann Surfaces (Williams & Wilkins, Baltimore, 1974).
[32] B. Runge, Quasihomogeneous singularities, Math. Ann 281 (1988) 295–313.
[33] B. Runge, On Siegel modular forms, part I, J. Reine Angew. Math. 436 (1993) 57–85.
[34] B. Runge, On Siegel modular forms, part II, Nagoya Math. J. 138 to appear.
[35] B. Runge, The Schottky ideal, Proceedings Abelian Varieties Egloffstein 1993, to appear.
[36] R.P. Stanley, Hilbert functions of graded algebras, Adv. Math. 28 (1978) 57–83.
[37] R.P. Stanley, Invariants of finite groups and their applications to combinatorics, Bull. Amer. Math. Soc. 1,3 (1979) 475–511.
[38] R. Weissauer, A remark on weight polynomials and self-dual even codes, unpublished.
[39] W. Wirtinger, Untersuchungen über Thetafunctionen (Teubner, Leipzig, 1895).
[40] E. Witt, Eine Identität zwischen Modulformen zweiten Grades, Abh. Math. Sem. Univ. Hamburg 14 (1941) 323–337.